STRATEGY RESEARCH PROJECT

MANAGING THE INTELLIGENT INFORMATION GRID FOR THE ARMY AFTER NEXT

BY

LIEUTENANT COLONEL P. T. HENGST
United States Army

USAWC CLASS OF 1997
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

MANAGING THE INTELLIGENT INFORMATION GRID FOR THE ARMY AFTER NEXT

by

LTC P.T. Hengst

Colonel Marland Burckhardt
Project Advisor

U.S. Army War College
Carlisle Barracks Pennsylvania 17013

ABSTRACT

AUTHOR: Paul T. Hengst (LTC), USA

TITLE: Managing the Intelligent Information Grid for the Army After Next

FORMAT: Strategy Research Project

DATE: 1 April 1997 PAGES: 34 CLASSIFICATION: Unclassified

In 2025, information superiority will be critical for the Army After Next (AAN). The key to this superiority will be the system of systems that make up the Intelligent Information Grid (I^2G). The I^2G will have two major components, communications systems and information systems. Because of government funding and manpower constraints, the communications systems will be primarily commercial based systems. Military unique communications systems will be limited. Information systems will be predominately commercial based software packages with military unique interfaces. The I^2G will be managed from CONUS by a consortium of commercial service providers and military personnel. Substantial intelligence will have to be built into the management system to meet the limited manpower objective. Critical management functions on the I^2G will be configuration control, access control, security and repair. A limited forward management function will be available for deployable units. A I^2G concept will be the only way to link the various sensors to databases and application programs to insure the common battlefield picture necessary in the AAN. The I^2G will have an evolutionary development from the array of communications and information systems currently used by the services.

TABLE OF CONTENTS

INTRODUCTION 1

WHAT THE I^2G MAY LOOK LIKE 1

WHAT TO MANAGE 8

WHO MANAGES THE I^2G 13

WHERE TO MANAGE THE I^2G 15

IMPLEMENTATION CONCERNS 16

CONCLUSIONS 20

ENDNOTES 23

GLOSSARY 27

SELECTED BIBLIOGRAPHY 29

Information superiority will be a key tenet in the Army After Next (AAN).[1] To achieve this superiority, the AAN will rely on information networks. These networks will be combined to form "a single grid so powerful and intelligent that it will be able to provide common situational awareness to friendly forces, real-time intelligence on enemy forces and fire control."[2] This intelligent information grid (I^2G) will be capable of connecting the multitude of sensors and information systems together in a seamless information environment.

The expected decreases in Department of Defense (DoD) funding and manpower are driving planners to develop a grid that will operate in a "management-by-exception mode without human interface."[3] This change will be a tremendous departure from our current network management techniques where thousands of soldiers, civilians and contractors perform the day-to-day network management functions. The purpose of this paper is to examine the I^2G needed for the AAN, how it will be managed, and the development challenges.

What the I^2G May Look Like

The best example of what the I^2G of the AAN should look like is the human nervous system. The human nervous system is a remarkable information-sensor network. A network of hundreds of miles of nerves run through the body connecting all of the major sensory centers. The sensors and nerve network work in harmony to develop a total awareness of an individual's surrounding. Within this network, the brain acts as a central computer and the spinal cord is the backbone of the network. Connected to the spine are the various major nerve bundles that provide the path for sensory inputs to

travel to the brain. This complex network quickly foresees any problem and is able to respond to any threat. Should a major attack on a component of the network occur, like an injury, the brain automatically responds to correct the error or limit the damage. The network of nerves can also be self healing when minor damage occurs. This nervous system to I^2G analogy is strong enough that some AAN planners have described the network as a "living internet."[4]

The future challenge is developing control mechanisms in the I^2G that are similar to our nervous system. Unlike the homogenous, single, connected network of the human-body, the AAN will still be operating under a system-of-systems concept.[5] Under this concept, multiple systems will exist and be connected together. The number of individual systems can be divided into two major areas, communications systems and information systems. The information age has blurred the distinction between these once separate and distinct areas. For clarity in describing the I^2G, each area will be discussed as a separate entity.

Communications systems. The human nervous system can be broken down into it's component parts, such as the brain, spinal cord, and nerves. Similarly, the communications systems integral to the I^2G can be broken into three key components. First is the backbone system, analogous to the spinal cord and major nerve bundles, capable of carrying high capacity of information. The second area is the local systems that extend from the backbone to the user or the individual nerves. The final area is the switching or transfer of signals between local and backbone systems.[6]

Backbone Systems. The backbone network will be comprised of the major communications systems we use today; satellites, microwave, and cable. No major

technological leap is predicted for backbone systems. However, developing technology will drive these systems to ever increasing bandwidth. This will be necessary to handle the volume of traffic expected to travel over the backbone network.

Satellites will become increasingly important in the AAN for two major reasons. First, is the flexibility to move fairly quickly to extend the backbone to areas without terrestrial systems and second, to cover large geographic regions with a single platform. Additionally, evolving compression techniques will increase bandwidth. However, transmission delays due to distance will still be a limiting factor for satellites.

The bulk of the terrestrial backbone will continue to ride over microwave and cable systems. Like satellites, technology will continue to push terrestrial systems to handle larger bandwidths. The current trend to replace copper-based cable with fiber optic cable will increase available bandwidth.[7]

Like our current force, the AAN will contract with commercial vendors to provide the bulk of the backbone systems.[8] This is primarily for economic reasons. First, the expected budget constraints of the future will not allow us to install, operate and maintain global communications networks. Second, we cannot afford the technology upgrades necessary to remain state-of-the-art. Finally, required manpower to operate and maintain backbone systems will exceed what we can afford. In addition to the economic benefit of contracting, an infrastructure based on commercial standards will help ensure interoperability within the defense community, other branches of government, and our allies.

Local Systems. Local systems connect user systems, such as voice and data networks, to the backbone. Like the backbone, we will continue to use those types of

systems in use today; line-of-sight radio, cable, single channel satellites, and cellular systems. Increases in bandwidth are also expected in local systems. There will be a continuing trend toward commercial systems at this level. Military unique systems will fill niche or unique requirements unavailable from commercial vendors.

The predominate local communication system in the AAN will be cellular. This is for two major reasons. First is the portability of communications.[9] Using a combination of terrestrial and projected space-based cellular systems, like Iridium,[10] cellular technology will offer the flexibility necessary to communicate in widely dispersed, fluid, operations. The second reason for cellular is that it offers a cheap alternative to installing a permanent cable-based infrastructure.[11] This is especially critical for contingency operations in lesser developed nations. Using local and space based cellular systems will also reduce the "rolling stock" infrastructure equipment and manpower we currently use on deployments.

Switching. Unlike backbone and local systems which will see a technological evolution to better, higher bandwidth systems, switching will undergo two major technological leaps. These are the combination of analog and digital switching and the communications unmanned aerial vehicle (UAV).

The development of a single device to quickly switch both voice and data will greatly reduce the infrastructure burden. Currently, we run parallel switched networks; analog for voice and digital for data. The cost of both equipment and manpower will make these parallel networks unaffordable in the AAN. Additionally, parallel networks will complicate the information sharing necessary to create common situational awareness. Technological improvements will also increase switching speed, especially

with the availability of optical switches.[12] Switching speed will be critical to prevent the switch from becoming the bottleneck or chokepoint for information traversing the network

The second technological leap in switching is the communication UAV. Used in a pseudo-satellite role, UAVs will be used as relay/switching stations between networks. Future enhancements, like in-flight refueling, will increase loiter time making UAVs candidates to supplement or replace existing military communications satellites. Additionally, these UAVs could provide the switching link from terrestrial cellular systems to the space backbone, particularly for deployments outside the normal commercial satellite footprint.

In summary, the communications systems of the AAN can be characterized as a commercial based system augmented by military assets to create a system-of-systems grid. The predominate communications architecture at the local level will be a cellular system based on commercial standards and protocols. Maximum use will be made of space based communications platforms. New technological developments will be integrated into an increasingly fiber optic based infrastructure.

Information Systems. The five senses; smell, touch, taste, sight, and hearing comprise the sensors of our human system. Input from the sensors is combined with the brain's stored knowledge to help us make decisions. In the AAN, information systems will include the full range of sensors, automated decision support tools, and databases working in a common operating environment to aid commanders in decision making. The processes used by our brain to make these decisions are analogous to application programs.

Common Operating Environment (COE). The development of the COE will be critical to prevent some of the information systems problems we currently experience. A COE provides a common look, touch, sound and feel to the user. Additionally, the COE ensures the interfaces from platform to platform are consistent.[13] The COE attempts to create a homogenous environment, much like our nervous system, where data is defined and shared easily between systems. This contrasts with our current information systems which are often a hodgepodge of stovepiped systems incapable of sharing all the data collected by the sensors. In order to obtain a common picture of the battlespace and take advantage of the vast amounts of data being collected, we must have systems that are totally interoperable and capable of sharing collected data. To insure this interoperability, the COE will establish standards for a wide range of items, to include; operating systems, communications protocols, and individual data elements.

Applications. The types of applications working in this COE will be numerous and largely commercially based. Applications will range from military unique command and control applications to administrative/office applications. For the most part, we will rely on the commercial software industry, not military software development centers, to provide the AAN the necessary applications. This is due to several interrelated factors; such as cost, development time, manpower, and training of software engineers. However, some applications will require military unique interfaces to be developed.

The bulk of the applications developed will be systems that collect information from a variety of databases. These databases will be built from the vast number of sensors expected to be in the AAN information environment. These databases will be linked via the I^2G to ensure information availability.

These interconnected databases will lead to an increasing amount of battlespace information available to the commander. Research has begun in trying to solve possible information overload problems.[14] Two intertwined concepts, datamining and digital agents, will come to fruition in the AAN to assist commanders in grappling with the information overload problem. Additionally, the growing use of simulation will aid the commander in testing courses of action and options prior to making any final decisions.

Datamining is the ability to take advantage of the vast amounts of data being collected and stored in various, often unrelated databases. The surface of this area is just now being scratched in military applications. In the commercial sector, one use of datamining is to determine individual buying patterns. A grocer may determine that most customers who purchase a particular snack food always buy the same type of soda and they purchase the items late in the week. By placing the two items close together or combining them in a package, the grocer may increase his sales. The grocer also establishes delivery dates for both items late in the week to reduce the amount of time he has to warehouse the items. All of this data is gathered when the items are scanned at the point of purchase. Using datamining concepts, logistic units can use similar techniques to determine key item delivery dates. Operational units can use datamining to correlate data from multiple sensors to establish possible patterns, both ours and the enemy's.

Digital agents will also assist the commander in handling information overload. Digital agents are described as "computer surrogates that possess a body of knowledge both about something (a process, a field of interest, a way of doing) and about you in relation to that something (your taste, your inclination, your acquaintances)."[15] With the perceived glut of information available to the commander, the use of digital agents will

assist him in building a profile of critical information requirements necessary for decision making. The use of digital agents could also reduce the human staffs that now collect and store this critical data.

The final piece to assist the commander in information overload is simulation. The non-linear battlefield has too many variables for most commanders to assimilate all the associated factors and conditions that may occur.[16] Simulation will allow commanders to pull information into the simulator, test the assumptions, and help determine the critical factors to success prior to conducting any operation. Simulations will be able to take into account the multitude of factors in a non-linear problem that linear database searches used by datamining or digital agents can not determine. Additionally, the visual nature of simulations assists the commander in retaining information.

The I^2G then, will consist of commercial-based communications systems at the backbone and local level. The communication systems will link the various components, sensors, databases and application programs into a system-of-systems. Intelligent applications connected by the I^2G will greatly assist the commander in decision making.

What To Manage

Now that we have an idea of what the I^2G may look like, it is necessary to determine what functions within the grid need to be managed. As mentioned in the introduction, the goal is a grid that requires a minimum amount of human intervention. This implies that a certain amount of intelligence must be built into the systems that make up the I^2G. With the unfulfilled promises of artificial intelligence (AI) over the past

twenty-five years, it is unlikely that AI will progress in the next twenty-five years to where no human intervention is required. Therefore, we will still use a combination of artificial and human intelligence to manage the major functions of the I^2G. In particular, those functions will be configuration control, security, and repair.

Configuration Control. There are three major configuration control areas; architecture, device addressing and bandwidth.

Architecture. While perhaps not a real time management feature, many of our current problems in network management are born from a lack of architectural control. Once again it is possible to look at the nervous system as an example. One of the great beauties of the human body is that underneath the skin we are pretty much alike. This is not true for our current information and communication systems. By not having a standard system architecture, we often rely on one or two gurus who understand how our systems work. If a problem occurs and the gurus are gone, nothing happens until they return. To overcome this problem, a standard architecture must be adopted. The Army has recently published the Army Technical Architecture (ATA) to help standardize the way we put networks together.[17] The ATA is also being used as the base line for the development of a Joint Technical Architecture.[18] This will help ensure interoperability in the joint information environment.

Device Addressing. The second issue of configuration control is knowing what devices are in the network, such as; satellites, switches, routers, computers, weapons platforms, and sensors. The expected fluid nature of warfare in the AAN requires devices that are self-addressing. Current manpower intensive addressing schemes, such as call signs on a given radio net, a phone number, or an Internet Protocol (IP) address, will be

unacceptable in an era of reduced manpower. Maximum use will have to be made of intelligent devices capable of registering themselves in the I^2G.

Bandwidth. The final aspect of configuration control is bandwidth. By controlling the configuration of the connected devices, the grid should be able to self-configure to ensure necessary bandwidth is available to all users. As noted in the communication system description, available bandwidth is expected to increase in the AAN. However, it will still be possible that multiple devices could overwhelm a particular link, which would decrease performance for all users on that link. Although irritating today when lack of bandwidth slows down our processing, it could become life threatening in the AAN when soldiers and weapons platforms are waiting for critical intelligence or "shooting" data. Therefore, certain platforms and sensors will have to receive priority for the available bandwidth with administrative traffic riding in the holes between priority traffic.

In summary, configuration control will be provided by a common grid architecture, the addressing scheme of the device and finally the allocation of bandwidth across the grid. Critical to the success of configuration control is a certain degree of intelligence built into the network to achieve the objective of minimum human intervention.

Security. The second major function to manage is security. Like configuration control, this function must require the minimum amount of manpower. The three major security items that require management are access security, information assurance and infrastructure protection.

Access Security. Unlike our current security protection architecture where we build separate systems of different security classifications, in the AAN we will have one grid with access security being provided at the "point-of-entry." This is not a new concept and is used in our current voice networks. For example, the STU-III telephone connected to a commercial line off-post is just as secure as when it is connected to a government owned line on an installation. Point-of-entry security is now being developed for a variety of devices, to include cellular telephones[19] and computers.[20] Point-of-entry security implies that we will have achieved a certain degree of multilevel security (MLS), which allows a single computer to operate at multiple security levels. The planned battlefield combat identification system (BCIS) for the identification of friendly vehicles can be used as a model for access security. Under this scheme, a device would enter the grid, be queried for it's address and routing information, identified as an authorized device and then be connected to the I^2G.[21]

Information Assurance. The second area of security is information assurance. We must retain the ability to protect the information we are using. Information assurance has four elements; availability, integrity, confidentiality, and non-repudiation.[22] Availability assures access to information by authorized users. Integrity protects the information from unauthorized change, while confidentiality protects the information from unauthorized disclosure. Finally, non-repudiation is the undeniable proof that users are who they say they are. Loss of information assurance will make all data suspect and would be catastrophic to an Army that relies on information to maintain battlefield dominance.

Infrastructure Protection. The final security area is infrastructure protection, currently addressed as command and control warfare (C^2W) in Army Information Operations terms,[23] or as Defensive Information Operations in Joint terms.[24] Infrastructure protection is the ability to protect the grid from attack and take over. The importance of this issue is realized and was the driving force behind the recently established President's Commission on Critical Infrastructure Protection.[25] The commission will examine the "cyber" threats to the national telecommunications infrastructure. If used properly, the output of this commission will result in shared responsibility between government and the commercial sector to provide adequate infrastructure protection. This shared responsibility will be critical to a military dependent on commercial communications systems.

Repair. The final function to manage is repair. The repair of the I^2G follows the healing process of our body, some repair is self-healing and some requires external intervention. Similar to configuration control and security, manpower to perform repair functions must be kept to a minimum. The loss of manpower combined with the increasing complexity of network repair will pose an interesting challenge to AAN.[26]

The complexity of repair will reduce most local maintenance to no more than item/board replacement. Diagnostic work will be accomplished through the grid by a centralized maintenance facility with the intelligent tools capable of analyzing the full range of possible alternatives. Individual platforms will have some limited self-diagnostic capability, but it is unlikely that crew members on informational weapons platforms like Crusader or Commanche will be able to do more than board level replacement.

Like other management functions, the diagnostic repair tools will require some degree of artificial intelligence. The greatest technological leap in this area will be in the tools to not only find the problem, but to correct the problem without human intervention. These maintenance tools would automatically create a log of their actions. The log would be reviewed by maintenance personnel in conjunction with other intelligent tools to take further action. For example, the grid diagnostic tool would notice a network laser at a remote unmanned communication node was pulsing too fast. Automated maintenance tools would take the laser out of service and activate the back-up. The action would be recorded in the log and the automated maintenance supervisor tool would prompt the repair person to physically replace the bad laser with a new one. For catastrophic problems, the automated maintenance supervisor would call or page the on-call repair person to immediately perform the necessary repair.

While we may never fully get away from some manpower requirements, like hardware replacement, most of the maintenance functions of the I^2G must be self-repairing. Intelligent programs, able to identify errors and take corrective measures to repair the damage, are critical in this area.

Who Manages the I^2G

After identifying what we will manage, the grid and individual functions, it is necessary to determine who will do the managing. When asked who controls your body, most of us would state, "I do." But what makes up the "I" in the grid will not be replicated by a single entity as our brain does for our body. Like today, the I^2G will be

managed from a variety of sources, some managing global functions, other managing local functions.

There will be two factors driving the who, jointness and manpower. The distinct roles and missions of each service results in almost all operations being joint. This will not change for the AAN. Therefore, all service elements will require interoperable systems that are managed by a joint force, although it will probably not be the Joint Information Corps proposed by some authors.[27] The required level of interoperability and management capability will drive the services towards joint solutions.

The reduction of manpower will manifest itself in some type of consortium of commercial vendors and military units. These two factions will be combined in a virtual operations cell to manage the function of the grid. Given the current state of deregulation, there may be a number of service providers in the operations cell. The consortium will conduct a variety of tasks, from day-to-day operations to standards setting. Military personnel will monitor the commercial networks and establish priorities between them.

The consortium concept will steadily evolve from the way we currently do business. The number of contractors used to assist military communicators is increasing. Both the Gulf War and the Force XXI demonstrations have shown the utility in using contractors to supplement military communications management.[28]

The development of a consortium to mange the I^2G in the AAN will be an evolutionary process. Continued reliance on commercial vendors to perform a variety of tasks, such as logistics, maintenance, and communications, will make this concept more acceptable. Additionally, joint military and commercial efforts, like the previously

mentioned President's commission on critical infrastructure, will help develop relationships necessary to support the transition to the consortium concept.

Where To Manage The I^2G

Thus far we have examined what to manage in the grid and who will do the management. It is also necessary to examine where we will manage the grid. Unlike the human nervous system, there will not be a single centralized management center. More likely, the widely dispersed system-of-systems will be managed at different locations with each location having visibility into all the other systems.

The majority of these management or consortium centers will almost certainly be located in the continental United States (CONUS). However, recent efforts to complete "a global pact that would phase out monopolies and restriction on competition" across the world-wide telecommunications industry may result in some centers residing in other countries.[29]

Military management centers will also be in CONUS. These centers can be co-located with commercial vendors, but more likely will reside on existing installations with communication links to the commercial centers. Based on the amount and type of service being contracted, liaison officers may be co-located with the commercial vendor.

A capability to establish deployable forward mini-centers will exist. These mini-centers will give commanders on the ground the ability to reallocate scarce resources and have limited control over portions of the grid, especially if the grid is established in a remote area. Additionally, local grid managers will have the capability of keeping the system running if cut off from CONUS based management centers. However, primary

management responsibility will remain with the CONUS centers. This supports taking in the smallest force - reducing the foot print - being able to quickly mass, complete the mission, and disperse the force.

In an age of information warfare (IW), where borders no longer matter and asynchronous attacks against our system are expected, the lack of one central control location will be to our advantage. This de-massification of network management will enhance the redundancy and survivability of the grid.

Therefore, the majority of network management functions for the I^2G will be controlled from CONUS centers in tightly coupled military-commercial management structure. The military will continue to maintain some type of deployable centers with limited ability to manage local assets.

Implementation Concerns - Are We Headed in the Right Direction

Some of the changes predicted above are built on evolutionary change (use of commercial vendors), while other changes may be more revolutionary (UAVs). The concerns about the success of these concepts can be broken down into two broad areas, technology and management.

Technology. There are three technological areas that will need to improve if the I^2G is to be constructed and managed as predicted above. First is improvement in artificial intelligence. For almost forty years, there has not been significant advances in producing artificial intelligence.[30] Some progress has been made around the edges with fuzzy logic and pattern recognition, but true intelligence replicating human analytical

reasoning has not occurred. The I^2G as described above requires significant artificial intelligence capabilities, particularly self-repair and access control.

The second technological area is multilevel security. Like artificial intelligence, much has been promised with very little result. Some products, like the multilevel security PC card FORTEZZA, may lead to a break-through in this area. Without multilevel security, the necessary security at the point-of-entry may be more difficult.

The final technological area is database technology, particularly those areas that support datamining and warehousing. It will be critical in the AAN to wrap all the sensor information into a framework understood by the decision maker. Without improvement in the database area, data will be collected and stored, but commanders will be unable to use it. While the use of digital agents may assist in this area, there is also a downside to their use. As we often collect information about one topic, we often discover information about something else that adds to our knowledge. By limiting the amount of information to just the few items a digital agent gathers, it may be possible for the commander to miss other information that could impact on his decision.[31]

Management. There are three major concerns with the management of the I^2G; reliance on commercial systems, funding and necessary future decisions.

Commercial Systems. As stated above, the I^2G will rely predominately on commercial systems. While this is not a great leap from where we are today, changes in the nature of the telecommunication business, such as global business groups and deregulation, will greatly change the way we interact with the vendors. The critical point is how the business world responds to what the military perceives as a crisis situation. As we discovered in the Gulf War, we can not always adequately predict what assets we will

need.[32] If limited assets are available, service providers may have to choose between military units and commercial customers. The commercial customer often has a bigger "checkbook" than the military. Providers that work in an open market will have a tough decision whether to increase profits or support a crisis. This becomes particularly challenging as telecommunications companies take on a more multi-national role and patriotism is diffused among a number of nations. This may result in changes to the law or contracting mechanisms to support military requirements in times of crisis. A program similar to the Air Force CRAF program for communications is another possible option.

Funding. The second management concern is funding. We rely on commercial systems because we can not afford to replicate the global networks vendors have built. This will not change in the future and places us as another customer in the open market. Vendors will continue to find new and unique ways of billing, which could increase our overall information costs. This is particularly true for funding contingency operations, where contractual agreements may not exist. Sufficient funding will be necessary to take advantage of technological gains and in some military unique cases push research. Trying to balance manpower, technology and systems fielding will be difficult with limited funding. However, the recent decision by DA DCSOPS to skip a generation of equipment and concentrate on information technology should assist in focusing available funding.[33] Finally, funding must be made available to upgrade our installation infrastructure, especially replacing copper and lead cable unable to handle the expected bandwidth requirements of future information systems.

Necessary Future Decisions. The final management area concerns future decisions that must be made. These decisions include; development responsibility, acquisition, risk, interoperability, and training.

The overall requirement to develop an I^2G must be assigned to one organization. Currently each service and DoD agencies are working on unique systems. However, these efforts are often not coordinated. Defense Information System Agency (DISA) or Assistant Secretary of Defense C3I may be in the best position to pull the individual efforts together. Part of this effort would be to continue the current move towards the establishment of a Joint Technical Architecture.

The I^2G will not come to fruition until the acquisition/procurement problem is fixed. Given a twelve to eighteen month life span of most computer related equipment, the time required to acquire state-of-the-art information technology is unacceptable. Strides have been made with the procurement of commercial-off-the-shelf (COTS) products. If we continue to use our current methods, information technology will continue to outpace our ability to put the latest technology in the hands of the soldiers. Additionally, leaders and managers must accept some individual responsibility for funding upgrades instead of waiting for everything to be pushed down from higher levels.

The senior military leadership will have to accept the risk of using commercial systems or agree to fund the building of a separate communications infrastructure. The crux of the problem is weighing the potential information warfare (IW) threat versus the billions of dollars it may take to build a global system. Agreeing to build separate systems will be expensive, in both equipment and manpower, but significantly lowers IW

risk. Complicating the decision is trying to determine if an IW attack constitutes an attack on the homeland and if it necessitates a military response.

To improve interoperability, tactical communication systems, like Mobile Subscriber Equipment (MSE), must be made to work smoothly with commercial systems. This requires not only some equipment/technological changes, but policy changes as well. Multilevel security equipment expected to be fielded in the next five to ten years should help to resolve the policy issue of classified networks being connected to unclassified networks. Seamless communications from deployed locations to the CONUS installations can not truly be accomplished until the link between tactical and commercial systems is fixed.

The final issue that must be addressed is training. One author has called for the immediate training in knowledge-based warfare "to soldiers, sailors, marines, and airmen at all levels of professional military education."[34] This is necessary if we are to understand not only how to operate and maintain the I^2G, but to also take advantage of the opportunity it offers in the way of information operations.

Conclusions

The AAN will require an I^2G capable of supporting the commander's information needs. The human nervous systems provides the architects of the I^2G the best example of what the grid should be. It should be a self-controlling and self-healing grid that users can plug into anywhere in the world. Technology will not fully take care of all grid management requirements. Therefore some type of human intervention will be necessary, but must be kept to a minimum in light of expected dwindling resources.

The critical functions the I^2G must manage include architecture, device addressing and bandwidth. Of these, architecture may be solved in the not too distant future when all services will be using a common joint architecture developed from the Army Technical Architecture model. Device addressing will be critical to quickly linking the full array of sensors, information systems and communication devices to the grid. Progress will have to be made in database technology to fully solve the device addressing issue. Finally, bandwidth may no longer be a problem as new techniques and mediums increase the amount of available bandwidth. However, in crisis or outages, bandwidth will still have to be managed and allocated to high priority users.

Security will continue to be a major concern in the AAN. Particularly as a society and Army, we become ever increasingly reliant on information technology. The threat of an asymmetrical attack against our information systems will continue to drive security technology. Of particular concern is the access security necessary to validate each device in the network and the assurance that the information is secure. Finally, we must protect the infrastructure from attack.

The I^2G will be managed by a consortium of business and military personnel from locations primarily in CONUS. We will continue to rely on commercial communications systems to provide the bulk of our communication requirements. The amount of change in the telecommunications business will drive us to establish new ways of doing business. Included in this may be new laws or contracts that provide for the reallocation of critical communication infrastructure in times of crisis.

The proposed management of the I^2G comes with some concerns. Technological concerns over database technology, multilevel security and artificial intelligence may

delay the development of the I^2G. Additionally, without establishing working relationships with commercial vendors and the assurance of funding, the I^2G can not be realized.

The creation of an I^2G has already started with the linking of current communications and information systems. However, at best it could be described as conglomeration of often non-interoperable, manpower intensive systems unable to share information. This conglomeration must be turned into a seamless information grid capable of providing commanders with the necessary information tools to aid in decision making. All of this must be accomplished with the minimum amount of human intervention. Without an I^2G, the information dominance necessary to achieve success in the AAN will not be obtainable.

ENDNOTES

[1]"Information superiority is the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." John M. Shalilikashvili, GEN, Joint Vision 2010 (Washington D.C.: The Joint Staff, 1996), 16.

[2]TRADOC Annual Report to the Chief of Staff of the Army on Army After Next Project, (Fort Monroe, VA: TRADOC AAN Staff, June 1996): 13.

[3]Ibid, 13.

[4]The term "living internet" or internetted "living" system of systems is from the TRADOC AAN brief given to the USAWC AAN Class on 23 October 1996.

[5]William A. Owens, ADM, "The Emerging System of Systems," US Naval Proceedings Vol. 121/5/1,107 (May 1995): 37 and Thomas G. Mahnken, "War in the Information Age," Joint Force Quarterly Vol. 16 (Winter 1995-96): 40.

[6]Switching in this context takes in the entire range of switches, routers and other devices used to switch signals between systems.

[7]Vincent W.S. Chan, "All-Optical Networks," Scientific American Vol. 273, No. 3, (September 1995): 73 and David L. Osborne, Domestic Trends to the Year 2015, Forecasts for the United States (Washington D.C.: The Library of Congress, 1991): 190.

[8]Robert K. Ackerman, "Digital Formats Complicate Information Security Tasks," Signal Vol. 51, No. 6 (February 1997): 22.

[9]George I. Zysman, "Wireless Networks," Scientific American Vol. 273, No. 3 (September 1995): 71.

[10] When it becomes operational in 1998, the IRIDIUM system will provide portable, universal service through a constellation of 66 satellites in low earth orbit. Subscribers will use pocket-size, hand-held IRIDIUM telephones transmitting through digital facilities to communicate with any other telephone in the world. The IRIDIUM system is being financed by an international investor consortium to telecommunications and industrial companies. "IRIDIUM" available from http://www.computerreview.com /iridium.htm; Internet, access 15 March 1997 and "Totally Global, Global Mobile Personal Communications by Satellite Offers New Vision," (Iridium on line magazine Fall 1996); available from http://www.iridium.com/public/fall/pubcov.html; Internet; access 20 Feb 1997.

[11]Zysman, 70 and Sheldon Teitelbaum, "Cellular Obsession," Wired Ed. 5.01 (January 1997): 147.

[12]During the author's visit to Lucent technology center in Homdel, N.J was briefed on an all fiber switch that was being developed and Vincent W.S. Chan, "All-Optical Networks," Scientific American Vol. 273, No. 3, (September 1995): 73.

[13]Shawn Butler, David Diskin, Norman Howes, and Kathleen Jordan, "Architectural Design of the Common Operating Environment for the Global Command and Control System," IEEE Software Internet, http://www.computer.org/pubs/software/extras/butler/butler.htm, accessed 15 March 1997, p 8.

[14]Andrew C. Braunberg, "Brain's Affinity for Imagery Eases Information Overload," Signal Vol. 51, No 4 (December 1996): 49. Also see, Lawrence E. Casper, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens, and T. Lamar Willis. "Knowledge-Based Warfare: A Security Strategy for the Next Century." Joint Force Quarterly (Autumn 96 Number 13): 84.

[15]Nicholas Negroponte, Being Digital (New York: Vintage Books, 1995), 151.

[16]Thomas J. Czerwinski, "Command and Control at the Crossroads," Parameters Vol. XXVI, No. 3 (Autumn 1996): 126. Also see, Glenn M. Harned, COL, The Complexity of War: The Application of Non-linear Science to Military Science, Paper Submitted At the Marine Corps War College, (Quantico, VA: The Marine Corps War College, 5 June 1995).

[17]The Army Technical Architecture, Version 4.0, Executive Summary, (Washington D.C.: The Army Staff, 30 January 1996): 1.

[18]Address by LTG Otto Guenther, DISC4, The Army Staff to the USAWC Class of 1997 on 29 January 1997. The Joint Technical Architecture being developed by the Joint Staff will use the Army Technical Architecture as the base model.

[19]Sean Patrick Burgess, "Art of the Small Supplies Secure Cellular Voice, Data," Signal Vol. 51, No. 1 (September 1996): 60.

[20]"What is DMS," available from the DMS Program Manger at http://www.monmouth.army.mil/dms/whatis.htm and National Security Agency Multilevel Information Systems Security Initiative (MISSI) Program explained by Defense Information System Agency (DISA) at http://www.disa.expoqa3.html.

[21]Scott R. Gourley, "The Battlefield Combat Identification System," Army Vol. 47, No. 1 (January 1997): 52.

[22]The Joint Staff currently uses 5 elements, availability, integrity, identification and authentication. confidentiality, and non-repudiation. In the I^2G identification and authentication is accomplished by access security. The Joint Staff, Joint Doctrine for Information Operations (First Draft), JCS Pub 3-13 (Washington: The Joint Staff, 21 January 1997): III-2.

[23]Department of the Army, Information Operations, Field Manual 100-6 (Washington; U.S. Department of the Army, 27 August 1996): 3-5.

[24]JCS Pub 3-13, III-6.

[25]President William J. Clinton, Executive Order 13010, Critical Infrastructure Protection, July 15, 1996. Taken from the Federal Register: July 17, 1996 (Volume 61 Number 138) 37345. (Federal Register Online wais.access.gpo.gov)

[26]Solving individual network problems has become increasingly complex. With computers now being connected to networks or in some cases multiple networks, an individual problem could have one of four possible outcomes. The problem could be hardware, software, network or some combination of the three.

[27]Martin C. Libick, The Mesh and The Net: Speculations on Armed Conflict in a Time of Free Silicon, (Washington, D.C.: National Defense University, 1994): 52.

[28]Dennis Steele, "Countdown to the Next Century," Army Vol. 46, No. 11 (November 1996): 21.

[29]"US Keeps World Waiting on Communications Deal," Carlisle (PA) Sentinel, 15 February 1997, sec A, p. 3.

[30]Douglas B. Lenat, "Artificial Intelligence," Scientific American Vol. 273, No. 3 (September 1995): 80 and H.M. Collins, Artificial Experts: Social Knowledge and Intelligent Machines, (Cambridge, MA: The MIT Press, 1990): 3.

[31]Cliff Stoll in his book Silicone Snake Oil discusses at several points the topic of searching for information leading to other information. In particular, see Chapter 11, "Wherein the Author Considers the Future of the Library, the Myth of Free Information, and a Novel Way to Heat Bathwater," Silicone Snake Oil (New York: Doubleday, 1995): 173-214. Also see, Jaron Lanier, "My Problem with Agents," Wired Ed. 4.11 (November 1996): 157.

[32]Alan D. Campen, "Gulf War's Silent Warriors Bind U.S. Units Via Space," Signal Vol. 45, No. 12 (August 1991): 81.

[33]"Modernizing to Achieve a Capabilities-Based Force," DA DCSOPNS brief given to the Army Research Laboratory (ARL) on 18 February 1997 and further discussed with US Army War College AAN Students on a visit to ARL on 3 March 1997.

[34]Lawrence E. Casper, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens, and T. Lamar Willis, " Knowledge-Based Warfare: Security Strategy for the Next Century," Joint Force Quarterly (Autumn 1996): 89.

GLOSSARY

AAN	Army After Next
ASD-C^3I	Assistant Secretary of Defense - Command, Control, Communications and Intelligence
ATA	Army Technical Architecture
battlespace	components determined by the maximum capabilities of friendly and enemy forces to acquire and dominate each other by fires and maneuver and in the electromagnetic spectrum
BCIS	Battlefield Combat Identification System
common operating environment	an environment that provides a familiar look, touch, sound and feel to the commander, no matter where the commander is deployed; information presentation and command, control communications, computers, and intelligence system interfaces are maintained consistently from platform to platform, enabling the commander to focus attention on the crisis at hand; also called COE
CONUS	continental United States
COTS	commercial off-the-shelf
CRAF	Civil Reserve Air Fleet
critical information	specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure of unacceptable consequences for friendly mission accomplishment
C^2W	command and control warfare
HQDA	Headquarters, Department of the Army
DCS OPS	Deputy Chief of Staff for Operations
DISA	Defense Information Systems Agency

DoD	Department of Defense
FORTEZZA	Multi-level secure PC-Card for personal computers
information dominance	the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary
information warfare	actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (CJCSI 3210.1)
IP	Internet Protocol
I^2G	Intelligent Information Grid
MLS	multilevel security
MSE	mobile subscriber equipment
relevant common picture of the battlefield	the aggregate of data that is shared among all friendly forces on the disposition of friendly and enemy force; this data is used to build a tailored relevant graphic display for the warfighter that increases in detail shown as the echelon served is closer to the soldier; commonly called situational awareness
UAV	Unmanned Aerial Vehicle

(Some Glossary items were taken from Information Operations, FM 100-6, HQDA, Washington: August 1996).

BIBLIOGRAPHY

Ackerman, Robert K. "Battlespace System Offers Data Anywhere, Anytime." Signal Vol. 51, No. 5 (January 1997): 26-29.

_____. "Digital Formats Complicate Information Security Tasks." Signal Vol. 51, No. 6 (February 1997): 21-23.

Albers, David S. The Unintended Consequences of Information Age Technologies. Washington: The National Defense University, 1996.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" Comparative Strategy. Vol. 12 (Spring 1993): 141-165.

Barker, Patrick K., CPT. Avoiding Technologically-Induced Delusions of Grandeur: Preparing the Air Force for an Information Warfare Environment. United States Air Force Academy, 1996.

Birman, Kenneth P. and Robert van Rensse. "Software for Reliable Networks." Scientific American Vol. 274, No. 5 (May 1996): 64-69.

Braunberg, Andrew C. "Brain's Affinity for Imagery Eases Information Overload." Signal Vol. 51, No. 4 (December 1996): 49-51.

Burgess, Sean Patrick. "Art of the Small Supplies Secure Cellular Voice, Data." Signal Vol. 51, No. 1 (September 1996): 60-61.

Butler, Shawn, David Diskin, Norman Howes, and Kathleen Jordon. "Architectural Design of the Common Operating Environment for the Global Command and Control System." IEEE Software 1995. Internet http://www.computer.org/pubs/software/extras/butler/butler.htm. 15 March 1997.

Campen, Alan D. COL (Ret). "Rush to Information-Based Warfare Gambles with National Security." Signal Vol. 49, No. 11 (July 1995): 67-69.

_____. Gulf War's Silent Warriors Bind U.S. Units Via Space." Signal Vol. 45 No. 12 (August 1991): 81-84.

Casper, Lawrence E., Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens, and T. Lamar Willis. "Knowledge-Based Warfare: A Security Strategy for the Next Century." Joint Force Quarterly No. 13(Autumn 96): 81-89.

Caudill, Maureen and Charles Butler. Understanding Neural Networks, VOL 1 and VOL2. Cambridge, MA: The MIT Press, 1992.

Chan, Vincent W. S. "All-Optical Networks." Scientific American Vol. 273, No. 3 (September 1995): 72-76.

Clinton, President William J., Executive Order 13010, Critical Infrastructure Protection, July 15, 1996. Taken from the Federal Register: July 17, 1996 (Vol. 61 No. 138): 37345-37350. (Federal Register Online wais.access.gpo.gov).

Cohen, Eliot A. "A Revolution in Warfare." Foreign Affairs Vol. 75, No. 2 (March/April 1996): 37-54.

Collins, H.M. Artificial Experts, Social Knowledge and Intelligent Machines. Cambridge, MA: The MIT Press, 1990.

Czerwinski, Thomas J. "Command and Control at the Crossroads." Parameters Vol. XXVI, No. 3 (Autumn 1996): 121-132.

Daggat, Russell. "Satellites for a Developing World." Scientific American Vol. 273, No. 3 (September 1995): 94.

Department of the Army, Information Operations. Field Manual 100-6. Washington D.C.: U.S. Department of the Army, 27 August 1996.

Elkan, Charles. "The Paradoxical Success of Fuzzy Logic." IEEE Expert Vol. 9, No. 4 (August 1994): 3-7.

Englebrecht, Joseph A. Jr. COL, LTC Robert L. Bivins, MAJ Patrick M. Condray, MAJ Merrily D. Fecteau, MAJ John P. Geis II, and MAJ Kevin Smith. Alternate Futures for 2025: Security Planning to Avoid Surprise. Maxwell AFB, AL: The Air War College. 1996.

Fancher, Carol, H. "Smart Cards." Scientific American Vol. 275, No. 2 (August 1996): 40-45.

Fayyad, Usama M. "Data Mining and Knowledge Discovery: Making Sense Out of Data." IEEE Expert Vol. 11, No. 5 (October 1996): 20-25.

Gourley, Scott R. "Land Warrior." Army Vol. 47, No. 2 (February 1997): 57-58.

_____. "The Battlefield Combat Identification System." Army Vol. 47, No. 1 (January 1997): 52-53.

Harasim, Linda M. ed. Global Networks: Computers and International Communications. Cambridge, MA: The MIT Press, 1993.

Harknett, Richard J. "Information Warfare and Deterrence." Parameters Vol. XXVI, No. 3 (Autumn 1996): 93-107.

Harned, Glenn M. COL, The Complexity of War: The Application of Non-linear Science to Military Science. Paper Submitted At the Marine Corps War College, (Quantico, VA: The Marine Corps War College, 5 June 1995).

Hendler, James A. "Guest Editor's Introduction: Intelligent Agents: Where AI Meets Information Technology." IEEE Expert Vol. 11, No. 6 (December 1996): 20-23.

Hewish, Mark. "Wearable Information Tailored to Battlefield." Jane's IDR Extra Vol. 1, No. 11 (November 1996): 1-7.

Hummel, Robert L. "Eight Ways to the Future," Byte Vol. 21, No. 12 (December 1996): 85-88.

Johnson, Stuart E. and Martin C. Libicki. Dominant Battlespace Knowledge, The Winning Edge. Washington: The National Defense University Press, 1995.

Josephson, Edward H. and Raymond M. Macedonia. Fighting Smarter: Leveraging Information Age Technology. Arlington, VA: The Institute of Land Warfare, 1994.

King, David and Daniel O'Leary. " Intelligent Executive Information Systems." IEEE Expert Vol. 11, No. 6 (December 1996): 30-35.

Kline, David. " The Embedded Internet." Wired Ed. 4.10 (October 1996): 98-106.

Lanier, Jaron. "My Problem with Agents." Wired Ed. 4.11 (November 1996): 157-160.

Lenat, Douglas B. "Artificial Intelligence." Scientific American Vol. 273, No. 3 (September 1995): 80-82.

Libicki, Martin C. "What is Information Warfare?" Strategic Forum 28 (May 1995): 1-3.

_____. The Mesh and the Net. Washington: National Defense University, 1994.

Lusted, Hugh S. and R. Benjamin Knapp. "Controlling Computers with Neural Signals." Scientific American Vol. 275, No. 4 (October 1996): 82-87.

Maes, Patie. "Intelligent Software." Scientific American Vol. 273, No. 3 (September 1995): 84-86.

Mahnken, Thomas G. "War in the Information Age." Joint Force Quarterly Vol. 16 (Winter 1995-96): 39-43.

Metz, Steven, William T. Johnsen, Douglas V. Johnson II, James O. Kievit, and Douglas C. Lovelace, Jr. The Future of American Landpower: Strategic Challenges for the 21st Century Army. Carlisle, PA: U.S. Army War College, 12 March 1996.

Molander, Rodger C., Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War." Parameters Vol. XXVI No. 3 (Autumn 1996): 81-92.

National Defense University, Strategic Assessment 1996, Instruments of U.S. Power. Washington: National Defense University Press, 1996.

Negroponte, Nicholas. Being Digital. New York: Vintage Books, 1995.

Nye, Joseph S. and William A. Owens. "America's Information Edge" in War, National Policy and Strategy. Vol. I, ed. U.S. Army War College, 1996: 135-148.

Patterson, David A. "Microprocessors in 2020." Scientific American Vol. 273, No. 3 (September 1995): 62-67.

Petersen, John L. The Road to 2015: Profiles of the Future. Coret Madera, CA: Waite Group Press, 1994.

Osborne, David L. Ed. Domestic Trends to the Year 2015, Forecasts for the United States. Washington D.C.: The Library of Congress, 1991.

Owens, William A., ADM. "The Emerging System of Systems." U.S. Naval Proceedings Vol. 121/5/1,107 (May 1995): 35-39.

Reimer, Dennis J., GEN. "Information Operations (IO) Intent and Strategy," AUTODIN Message DTG 031948Z September 1996 from GEN Reimer, CSA, to Major Army Commands.

_____. Army Vision 2010. Washington, D.C.: The Pentagon. 1996.

Rennie, John. "The Uncertainties of Technological Innovation." Scientific American Vol. 273, No. 3 (September 1995): 57-58.

Robinson, Clarence A., Jr. ed. "Group Formed to Fight Cyberwar." Sub-article in NewsNet Feature. Signal Vol. 51, No. 1 (September 1996): 8-10

_____. "Tactical Wireless Links Free Highly Mobile Battle Forces." Signal Vol. 51, No. 4 (December 1996): 17-20.

_____. "Information Warfare Demands Battlespace Visualization Grasp." Signal Vol. 51 No. 6 (February 1997): 17- 20.

Rowe, Wayne J. Information Warfare: A Primer for Navy Personnel. Newport R.I.: U.S. Naval War College, 1995.

Shalikashvili, John M. Joint Vision 2010. Washington D.C.: The Joint Staff, 1996.

Simon, Alan. "Better Clients, Better Decisions." Byte Vol. 22, No. 1 (January 1997): 91-94.

Steele, Dennis. "Countdown to the Next Century," Army, Vol. 46, No. 11 (November 1996): 16-22.

Stoll, Clifford. Silicon Snake Oil. New York: Doubleday, 1995.

Strauss, Leonard. "Modern Surveillance Sensors." Signal Vol. 51, No. 3 (November 1996): 71-75

Sullivan, Gordon R., General and James M. Dubik, COL. War in the Information Age. Carlisle, PA: U.S. Army War College, 6 June 1994.

_____ and Anthony M. Coroalles, LTC. The Army in the Information Age. Carlisle, PA: U.S. Army War College, 31 March 1995.

Szafranski, Richard. "When Waves Collide: Future Conflict." Joint Force Quarterly. (Spring 1995): 77-84.

Teitelbaum, Sheldon. "Cellular Obsession." Wired Ed. 5.01 (January 1997):144-149 and 194-197.

The Army Technical Architecture, Version 4.0. Washington D.C.: The Army Staff, 30 January 1996.

The Joint Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington: The Joint Staff, 30 May 1995.

The Joint Staff. Joint Doctrine for Information Operations (First Draft). JCS Pub 3-13. Washington: The Joint Staff, 21 January 1997.

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little, Brown & Co., 1993.

TRADOC Annual Report to the Chief of Staff of the Army on Army After Next Project. Fort Monroe, VA: TRADOC AAN Staff, June 1996.

Van Creveld, Martin L. Command in War. Cambridge, MA: Harvard University Press. 1985.

_____. Technology and War. New York: The Free Press, 1989.

Waller, Douglas. "Onward Cyber Soldiers." Time. 21 August 1995, 38-46.

Wasserman, Philip D. Advanced Methods in Neural Computing. New York: Van Nostrand Reinhold, 1993.

Weldon, Jay-Louise and Alan Joch. "Data Warehouse Building Blocks." Byte Vol. 22 No. 1 (January 1997): 82-83.

Whisenhunt, Robert H. Information Warfare and the Lack of a U.S. National Policy, Carlisle, PA: U.S. Army War College, 1996.

Zysman, George I. "Wireless Networks." Scientific American Vol. 273, No. 3 (September 1995): 68-71.

"Totally Global, Global Mobile Personal Communications by Satellite Offers New Vision." (Iridium on line magazine Fall 1996); available from http://www.iridium.com/public/fall/pubcov.html; Internet; access 20 Feb 1997.

"US Keeps World Waiting on Communications Deal." Carlisle (PA) Sentinel 15 February 1997, sec A, p 3.